IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Application of:)
)
    Iyad Qumei)
)
Serial No. 10/813,212)   **Electronically Filed on**
)
Filed: March 30, 2004)
)   **August 20, 2008**
For: Electronic Device Network)
Supporting Enciphering And Deciphering)
And Update Generation In Electronic)
Devices)
)
Examiner: Chen, Shin Hon)
)
Group Art Unit: 2131)
)
Confirmation No. 4068)

REPLY BRIEF

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

This Reply Brief responds to the Examiner's Answer mailed June 23, 2008. Appellant respectfully requests that the Board of Patent Appeals and Interferences reverse the final rejection of all rejected claims of the present application for at least the reasons set forth in the Appeal Brief filed on April 3, 2008, and the following.

REMARKS

Appellant appreciates the withdrawal of the previously asserted rejections to claims 3, 13-21, 29, 39, and 40. Appellant further appreciates the statements in the Examiner's Answer indicating that claims 13-21 are allowed, and that 3, 29, 39 and 40 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. However, Appellant respectfully disagrees with the rejections of the remaining claims which were maintained in the Examiner's Answer. For at least the reasons discussed previously, for example, in the April 3 Appeal Brief, as well as the following, Appellant respectfully requests the reversals of the rejections maintained in the Examiner's Answer.

I. Selkirk Does Not Anticipate Claims 1, 2, 4-9, and 12

As pointed out previously, claim 1 recites "an electronic device network for updating at least one of firmware and software in a plurality of electronic devices using at least one electronic device update, the network comprising at least one update generator adapted to generate updates, the at least one update generator comprising an encrypting and decrypting engine; at least one update store storing a plurality of electronic device updates; at least one update delivery server adapted to dispense the plurality of electronic device updates; and **wherein at least a portion of the at least one of firmware and software in the plurality of electronic devices is encrypted.**" As detailed below, Appellant respectfully submits that Selkirk fails to disclose, at least, "wherein at least a portion of the at least one of firmware and software in the plurality of

electronic devices, is encrypted." Appellant has previously discussed the allowability of

claim 1 over Selkirk. (*See, e.g.,* Appeal Brief at p. 8-15).

The Examiner's Answer again cites the same portions of Selkirk as were

previously cited, namely paragraphs [009] and [0017]. (*See* Examiner's Answer at 5-6.)

Appellant respectfully submits that the cited portions of Selkirk do not properly support

an anticipation rejection, as explained, for example, in the Appeal Brief. In addition to

the earlier submissions regarding the allowability of claim 1 and its dependent claims

over Selkirk, Appellant also now addresses the response to those previous submissions

in the Examiner's Answer.

The Examiner's Answer, in asserting that Selkirk discloses "wherein at least a

portion of the at least one of firmware and software in the plurality of electronic devices

is encrypted" stated as follows:

> However, the examiner disagrees. The examiner has relied
> on the Selkirk reference to disclose securely transmitting
> encrypted firmware update from server to client and <u>no</u>
> <u>decryption of the encrypted firmware update takes place</u>
> <u>outside of the **firmware device**</u> (Selkirk: [0017] lines 18-25:
> <u>the **firmware update** is a portion of the firmware and</u>
> <u>software</u> of the electronic device). Therefore, when the
> firmware device receives firmware update/portion of the
> firmware and software in the electronic device, the firmware
> update is in encrypted state prior to decryption.

(Examiner's Answer at p. 12; emphasis added). Appellant respectfully submits that the

stated reasons in the Examiner's Answer do not support an anticipation rejection for

several reasons. Appellant respectfully submits that a <u>firmware device</u> and a <u>firmware</u>

<u>update</u> are quite different from the <u>firmware itself</u> in an electronic device.

For example, the Examiner's Answer improperly confuses "the firmware <u>device</u>" of Selkirk as "firmware." Appellant respectfully submits there is a clear distinction between firmware and a firmware <u>device</u>. Even if, *arguendo*, Selkirk did disclose an encrypted update present in the firmware device, that would not disclose wherein at least a portion of the at least one of firmware and software in the plurality of electronic devices is encrypted. The firmware device of Selkirk is not the same as firmware itself -- indeed, Selkirk describes its firmware device as comprising much more than just firmware:

> [0023] FIG. 2B is a block diagram depicting the structure of firmware device 108. An <u>embedded processor</u> 200B is embedded into firmware device 108 and functions as the control center for firmware device 108. Embedded processor 100B communicates through <u>internal bus</u> 202B with <u>cryptographic program memory</u> 204B, from which it loads instruction for it to execute. Also connected to device bus 202B is an <u>external bus interface</u> 206B, which allows embedded processor 200B to send and receive data through external bus 208B, which is associated with the computer or peripheral for which firmware device 108 supplies the firmware.
>
> [0024] <u>Firmware memory</u> 210B is connected to internal bus 202B and provides storage for <u>the actual firmware</u> (i.e., the code and data to be used by the computer or peripheral. Firmware memory 210B is preferably some kind of writeable non-volatile memory, such as flash ROM (read-only memory), and EEPROM (electrically-erasable read-only memory), or non-volatile RAM (random-access memory).

(Selkirk at [0023]-[0024]; emphasis added; *see also id.* at Fig. 2B; *see also id.* at [0017] lines 14-18: "firmware device 108 may be, for instance, a monolithic integrated circuit, but it may comprise any combination of hardware components, including discrete logic

circuitry, multiple integrated circuits, optical storage, and any other suitable storage medium.") Thus, Selkirk explicitly acknowledges the distinction between a "firmware device" and "the actual firmware." And Selkirk also makes clear that the update is decrypted before being stored in the firmware memory, where the "actual firmware" is stored. Selkirk describes the received encrypted file being decrypted <u>before</u> being stored in the firmware device.

> FIG. 5 is a flowchart representation of a process of receiving a data file by a firmware device from a server in accordance with a preferred embodiment of the present invention. First, the encrypted file is received by the firmware device (step 500). The file is decrypted by the firmware device (step 502). Finally, the firmware device stores the file (step 504).

(Selkirk at [0037]; *see also id*. at Fig. 5). Thus, because the file of Selkirk is decrypted <u>before</u> the firmware device stores the file, and because Selkirk states that the "actual firmware" is <u>stored</u> in "firmware memory 210B," Selkirk does not disclose "wherein at least a portion of the at least one of firmware and software in the plurality of electronic devices is encrypted." Instead, in Selkirk, an encrypted file is decrypted before it is stored and can become a part of the actual firmware. Thus, the assertions regarding purported encryption either in a "firmware <u>device</u>" or a "firmware <u>update</u>" do not address the presently claimed subject matter's recitation of encryption of at least a portion of the at least one of <u>firmware</u> and software.

The Examiner's Response also asserts that "although Selkirk does not disclose in detail generation of the update, paragraph [0017] provides sufficient information

pertaining to generation of firmware update as coming from the server which implies that the server is responsible for generation of the update." (Examiner's Answer at p. 13). Appellant respectfully disagrees with this assertion as previously discussed, for example in the Appeal Brief. Appellant further notes that the Examiner's Answer neither asserts inherency nor provides the requisite support for such an assertion, and that the asserted "implication" of a teaching to Selkirk does not properly support an anticipation rejection.

As a result of at least the foregoing, Appellant respectfully submits that the Examiner has failed to establish anticipation with respect to claim 1 or any claim that depends from claim 1.

II. Selkirk Does Not Anticipate Claims 22-28 and 30

As an initial matter, it is not entirely clear what grounds are being used to reject claims 22-28 and 30. The final Office Action stated, "As per claims 22-41, claims 22-41 encompass the same scope and obvious variation of claims 1-21. Therefore, claims 22-41 are rejected based on the same reasons set forth above in rejection claims 1-21." (Final Office Action at p. 8). The Examiner's Response, however, indicates that these claims are rejected as anticipated. In any event, Appellant respectfully submits that, for at least the reasons discussed in the Appeal Brief, these claims are neither anticipated nor rendered obvious by the cited art. (*See, e.g.*, Appeal Brief at 17-18).

For example, as Appellant has previously pointed out, the cited art is silent with respect to, for example, a first-in-first-out (FIFO) memory device, as claimed by claim 22. The Examiner's Response asserts as follows:

> Selkirk discloses the firmware memory is connected to internal bus and provides storage for the actual firmware and is preferably some kind of write-able non-volatile memory such as EEPROM, flash ROM and non-volatile RAM (Selkirk: [0024]). Therefore, although no specific word mentions "FIFO" and FIFO memory does not appears [sic] to be a patentable feature, the memory device disclosed by Selkirk discloses the hardware limitation disclosed by appellant. In addition, the claim only recites of a FIFO memory device but fails to distinguish how the FIFO is used in relation to updating of firmware.

(Examiner's Response at p. 13-14). Appellant respectfully submits that the above assertions do not properly support an anticipation rejection. For example, "some kind of write-able non-volatile memory" does not disclose a FIFO memory device.

In any event, Appellant further notes that claim 22 recites "wherein the electronic device is adapted to update an encrypted portion of at least one of the firmware and the software application selected for updating." As previously discussed, for example, in connection with claim 1 and its dependent claims, Selkirk does not disclose at least this aspect of the presently claimed subject matter.

As a result of at least the foregoing, Appellant respectfully submits that the Examiner has failed to establish anticipation or obviousness with respect to claim 22 or any claim that depends from claim 22.

III.   Selkirk Does Not Anticipate Claims 31 and 41

With respect to claims 31 and 41, the Examiner's Response asserts that Selkirk discloses "encrypting the components before assembling the components into an encrypted firmware image" because "Selkirk discloses that firmware update is subject to encryption and the encryption preferably uses RC4 cipher/stream cipher or DES/block cipher that encrypts data by performing encryption block by block/component by component (Selkirk: [0034]).   Therefore, the components of firmware update are encrypted prior to being assembled in to an update packet." (Examiner's Response at p. 14). Appellant respectfully disagrees.

As an initial matter, the cited portion of Selkirk does not explicitly recite, for example, "block by block" or "component by component" encryption. That portion of Selkirk reads as follows:

> [0034] Although SSL must rely on some form of public-key cryptography in its handshake procedure, SSL may use any of a number of cryptosystems (called "cipher suites" in SSL parlance) for data transmission. Cipher suites supported by SSL include DES (data encryption standard), 3DES (triple DES), DSA (digital signature algorithm), KEA (key exchange algorithm), MD5 (message digest algorithm 5), RC2 (Rivest cipher 2), RC4 (Rivest cipher 4), RSA (Rivest, Shamir, and Adleman) public-key algorithm, RSA key exchange, SHA-1 (secure hash algorithm) and SKIPJACK. Note that some of these cipher suites are suitable for handshaking, while others are suitable for data transmission. RSA is commonly used for handshaking, and RC4 is commonly used for data transmission, for example.

Thus, the Examiner's Response appears to be relying on some form of obviousness and/or inherency assertion, but has not supported that assertion. In any event, even if

the cited portion of Selkirk, which deals with "handshaking" and "data transmission," did disclose "block by block" or "component by component" encryption, that still would not disclose the subject matter of claim 31, which recites, for example, "encrypting the components before assembling the components into an encrypted firmware image." Appellant respectfully submits that encrypting components before assembling the components into an encrypted firmware image is different from, and not disclosed by, such "handshaking" or "data transmission."

As a result of at least the foregoing, Appellant respectfully submits that the Examiner has failed to establish anticipation or obviousness with respect to claim 31 or any claim that depends from claim 31.

IV.   **Selkirk and Nachenberg Do Not Render Claims 10, 11, and 32-38 Obvious**

Each of claims 10, 11, and 32-38 depend from allowable claims, as discussed above, and are therefore allowable for at least the same reasons as previously discussed above. Appellant further submits these claims are allowable for at least the reasons previously discussed, for example, in the Appeal Brief. (*See, e.g.*, Appeal Brief at p. 20). Appellant further submits that the Examiner's Response provides no support -- either by way of affidavit or citation to prior art -- of its assertions regarding certain procedures being "well known in the art," or support for how or why it would be obvious to use such procedures in the context of the presently claimed subject matter.

As a result of at least the foregoing, Appellant respectfully submits that the Examiner has failed to establish obviousness with respect to the above listed claims.

V.   Conclusion

Appellant respectfully submits that the pending claims of the present application should be in condition for allowance for at least the reasons discussed in the Appeal Brief and above.   Therefore, the Board is respectfully requested to reverse all of the present rejections.

Respectfully submitted,

Date: August 20, 2008   /Kevin E. Borg/
                                        Kevin E. Borg
Hewlett-Packard Company   Reg. No. 51,486
Intellectual Property Administration
Legal Department, M/S 35
P.O. Box 272400
Fort Collins, CO 80527-2400